

Docket No.: 60188-720

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of : Customer Number: 20277
Masanori MATSUURA : Confirmation Number:
Serial No.: : Group Art Unit:
Filed: November 26, 2003 : Examiner:
For: STORAGE DEVICE

CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Mail Stop CPD
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

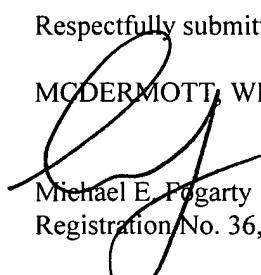
Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicant hereby claim the priority of:

Japanese Patent Application No. JP 2002-348774, filed on November 29, 2002

cited in the Declaration of the present application. A certified copy is submitted herewith.

Respectfully submitted,


MCDERMOTT, WILL & EMERY

Michael E. Pogarty
Registration No. 36,139

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 MEF:gav
Facsimile: (202) 756-8087
Date: November 26, 2003

60188-72Φ
Masanori MATSUURA
November 29, 2003

日本国特許庁 *McDeragh, Will & Emery*
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application: 2002年11月29日

出願番号 Application Number: 特願2002-348774

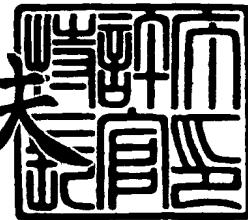
[ST. 10/C]: [JP 2002-348774]

出願人 Applicant(s): 松下電器産業株式会社

2003年10月22日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 5037740025

【提出日】 平成14年11月29日

【あて先】 特許庁長官 殿

【国際特許分類】 G06K 19/073

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地
松下電器産業株式会社内

【氏名】 松浦 正則

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100077931

【弁理士】

【氏名又は名称】 前田 弘

【選任した代理人】

【識別番号】 100094134

【弁理士】

【氏名又は名称】 小山 廣毅

【選任した代理人】

【識別番号】 100110939

【弁理士】

【氏名又は名称】 竹内 宏

【選任した代理人】

【識別番号】 100110940

【弁理士】

【氏名又は名称】 嶋田 高久

【選任した代理人】

【識別番号】 100113262

【弁理士】

【氏名又は名称】 竹内 祐二

【選任した代理人】

【識別番号】 100115059

【弁理士】

【氏名又は名称】 今江 克実

【選任した代理人】

【識別番号】 100115510

【弁理士】

【氏名又は名称】 手島 勝

【選任した代理人】

【識別番号】 100115691

【弁理士】

【氏名又は名称】 藤田 篤史

【手数料の表示】

【予納台帳番号】 014409

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0006010

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 記憶装置

【特許請求の範囲】

【請求項 1】

メモリとマイクロコンピュータとを備え、外部から入力されるクロック信号またはこれに基づいて生成されるクロック信号に応じて、上記メモリに記憶されたデータが上記マイクロコンピュータに取り込まれるように構成された記憶装置において、

上記メモリからの記憶データの読み出しを制御する読み出し制御信号における所定のエッジから所定の時間だけずれたタイミングを示すタイミング信号を出力するタイミング信号出力回路と、

上記タイミング信号に基づいて、上記クロック信号が少なくとも 1 つの所定の周波数の場合にだけ、上記メモリに記憶されたデータが上記マイクロコンピュータに取り込まれるように制御する読み出しデータ制御回路と、
を備えたことを特徴とする記憶装置。

【請求項 2】

請求項 1 の記憶装置であって、

上記読み出しデータ制御回路は、上記タイミング信号に基づいて、

上記メモリから読み出されたデータの上記マイクロコンピュータへの出力の有無、

上記メモリから読み出されたデータの上記マイクロコンピュータへの出力タイミング、および

上記マイクロコンピュータが上記メモリから読み出されたデータを取り込むタイミング

のうちの少なくとも何れか 1 つを制御するように構成されたことを特徴とする記憶装置。

【請求項 3】

請求項 2 の記憶装置であって、

上記読み出しデータ制御回路は、上記タイミング信号によって示されるタイミ

ングと、上記読み出し制御信号における上記所定のエッジよりも後のエッジが生じるタイミングとの相対関係に基づいて、上記メモリから読み出されたデータの上記マイクロコンピュータへの出力の有無を制御するように構成されたことを特徴とする記憶装置。

【請求項4】

請求項2の記憶装置であって、

上記読み出しデータ制御回路は、上記メモリから読み出されたデータを、上記タイミング信号に応じた所定の期間だけ、上記マイクロコンピュータへ出力するように構成されたことを特徴とする記憶装置。

【請求項5】

請求項2の記憶装置であって、

さらに、上記メモリから読み出されたデータを、所定の期間だけ、上記マイクロコンピュータへ出力するマスク回路を備えるとともに、

上記読み出しデータ制御回路は、上記マイクロコンピュータが、上記タイミング信号に応じた所定のタイミングで、上記マスク回路から出力されたデータを取り込むよう制御するように構成されたことを特徴とする記憶装置。

【請求項6】

請求項3から請求項5の何れか1つの記憶装置であって、

上記読み出しデータ制御回路、または上記マスク回路は、上記所定の期間以外には、上記メモリから読み出されたデータとは異なるデータを出力するように構成されたことを特徴とする記憶装置。

【請求項7】

請求項3から請求項6の何れか1つの記憶装置であって、

さらに、温度検知回路を備え、

上記読み出しデータ制御回路、または上記マスク回路は、上記温度検知回路によって所定の温度が検出されたときにだけ、上記メモリから読み出されたデータを出力するように構成されたことを特徴とする記憶装置。

【請求項8】

請求項3から請求項6の何れか1つの記憶装置であって、

さらに、光検知回路を備え、

上記読み出しデータ制御回路、または上記マスク回路は、上記光検知回路によって所定の強度の光が検出されたときにだけ、上記メモリから読み出されたデータを出力するように構成されたことを特徴とする記憶装置。

【請求項 9】

メモリとマイクロコンピュータとを備え、外部から入力されるクロック信号に応じて、上記メモリに記憶されたデータが上記マイクロコンピュータに取り込まれるように構成された記憶装置において、

上記メモリから読み出されたデータを、所定の期間だけ、上記マイクロコンピュータへ出力するマスク回路と、

上記マスク回路が上記メモリから読み出されたデータを出力する上記所定の期間、および上記マイクロコンピュータが上記マスク回路から出力されたデータを取り込むタイミングを可変に制御するタイミング制御回路と、
を備えたことを特徴とする記憶装置。

【請求項 10】

請求項 9 の記憶装置であって、

上記タイミング制御回路は、

上記マスク回路が上記メモリから読み出されたデータを出力する上記所定の期間、および上記マイクロコンピュータが上記マスク回路から出力されたデータを取り込むタイミングを、

上記メモリにおける所定の領域に保持されたデータ、

上記マイクロコンピュータから出力されるアドレス、および

上記マイクロコンピュータから出力される所定の信号の少なくとも何れか1つに基づいて設定するように構成されたことを特徴とする記憶装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、半導体メモリとプロセッサとを有するICカード等の記憶装置に関し、特に、上記半導体メモリに記憶されたデータの秘匿性を高める技術に属する

ものである。

【0002】

【従来の技術】

近年、マイクロコンピュータおよび半導体記憶部を備えた、例えばICカード等の記憶装置の市場は急速に広がりを見せ、様々な用途に応用されるようになって来ている。

【0003】

特に、個人データや金銭的なデータをICカード等に格納して用いる用途も普及しつつある。このような用途に用いる場合、内部に記憶されたデータの秘匿性が重要なものとなる。

【0004】

一方、ICカードの製造や運用をする企業などにとって、ICカードを開発する場合や、市場に出荷されたICカードに不具合が生じた場合などに、内部に記憶されているデータを読み出して解析等する必要が往々にしてある。

【0005】

このため、第3者が悪意にデータを読み出すことを防ぐとともに、ICカードの開発時などには容易に内部データを読み出せるようにすることが求められている。

【0006】

上記のような機密保持と解析等の容易化などとの両立を図る技術としては、例えば、ICカードに固有の番号を保持させ、ホスト装置から入力した番号と照合してゲート回路を開閉するものが提案されている（例えば、特許文献1参照）。

【0007】

また、記憶させるデータ自体を暗号化して、データが読み出されても容易には解読できないようにする技術も知られている。

【0008】

【特許文献1】

特開平6-139422号公報

【0009】

【発明が解決しようとする課題】

しかしながら、上記のように固有の番号を照合する手法は、万一、その番号が漏れた場合には無防備なものとなる。また、一連の番号が順次入力されることによって機密を破られるおそれもある。さらに、ICカードが分解され、配線にプロープが当てられて解析されるような場合にも、機密を保持することが困難である。

【0010】

また、データの暗号化が用いられる場合には、秘匿性は暗号強度によって決まるため、必ずしも高い秘匿性が得られるとは限らない。

【0011】

上記の問題に鑑み、本発明は、ICカード等の記憶装置の秘匿性を高めることができ、より容易にできるとともに、必要に応じて内部データを読み出すことなども容易にできるようにすることを課題とする。

【0012】**【課題を解決するための手段】**

上記の課題を解決するために、請求項1の発明が講じた解決手段は、メモリとマイクロコンピュータとを備え、外部から入力されるクロック信号またはこれに基づいて生成されるクロック信号に応じて、上記メモリに記憶されたデータが上記マイクロコンピュータに取り込まれるように構成された記憶装置において、

上記メモリからの記憶データの読み出しを制御する読み出し制御信号における所定のエッジから所定の時間だけずれたタイミングを示すタイミング信号を出力するタイミング信号出力回路と、

上記タイミング信号に基づいて、上記クロック信号が少なくとも1つの所定の周波数の場合にだけ、上記メモリに記憶されたデータが上記マイクロコンピュータに取り込まれるように制御する読み出しデータ制御回路と、を備えたことを特徴とする。

【0013】

請求項1の発明によると、クロック信号が所定の周波数でなければ、メモリに

記憶された記憶データはマイクロコンピュータに取り込まれず、記憶装置の外部に出力されないとともに、マイクロコンピュータも適切に動作しないようとすることができる。それゆえ、多くの場合に行われるような、低いクロック信号の周波数で不正に記憶データを解析したりする行為を防止して、記憶装置に記憶されたデータの秘匿性を高くすることが容易にできる。

【0014】

また、請求項2の発明は、

請求項1の記憶装置であって、

上記読み出しデータ制御回路は、上記タイミング信号に基づいて、

上記メモリから読み出されたデータの上記マイクロコンピュータへの出力の有無、

上記メモリから読み出されたデータの上記マイクロコンピュータへの出力タイミング、および

上記マイクロコンピュータが上記メモリから読み出されたデータを取り込むタイミング

のうちの少なくとも何れか1つを制御するように構成されたことを特徴とする。

【0015】

また、請求項3の発明は、

請求項2の記憶装置であって、

上記読み出しデータ制御回路は、上記タイミング信号によって示されるタイミングと、上記読み出し制御信号における上記所定のエッジよりも後のエッジが生じるタイミングとの相対関係に基づいて、上記メモリから読み出されたデータの上記マイクロコンピュータへの出力の有無を制御するように構成されたことを特徴とする。

【0016】

また、請求項4の発明は、

請求項2の記憶装置であって、

上記読み出しデータ制御回路は、上記メモリから読み出されたデータを、上記タイミング信号に応じた所定の期間だけ、上記マイクロコンピュータへ出力する

ように構成されたことを特徴とする。

【0017】

また、請求項5の発明は、

請求項2の記憶装置であって、

さらに、上記メモリから読み出されたデータを、所定の期間だけ、上記マイクロコンピュータへ出力するマスク回路を備えるとともに、

上記読み出しデータ制御回路は、上記マイクロコンピュータが、上記タイミング信号に応じた所定のタイミングで、上記マスク回路から出力されたデータを取り込むよう制御するように構成されたことを特徴とする。

【0018】

これらによると、前記のようにメモリに記憶された記憶データがマイクロコンピュータに取り込まれないようにすることができる。

【0019】

また、請求項6の発明は、

請求項3から請求項5の何れか1つの記憶装置であって、

上記読み出しデータ制御回路、または上記マスク回路は、上記所定の期間以外には、上記メモリから読み出されたデータとは異なるデータを出力するように構成されたことを特徴とする。

【0020】

これによると、やはり、クロック信号が所定の周波数でない場合に、記憶データがマイクロコンピュータに取り込まれることがないとともに、記憶装置を分解し、記憶データの伝送経路にプローブを当てて解析される場合などでも、正しい記憶データを識別することが困難であるため、やはり、不正な情報の取得を容易に防止することができる。

【0021】

また、請求項7の発明は、

請求項3から請求項6の何れか1つの記憶装置であって、

さらに、温度検知回路を備え、

上記読み出しデータ制御回路、または上記マスク回路は、上記温度検知回路に

よって所定の温度が検出されたときにだけ、上記メモリから読み出されたデータを出力するように構成されたことを特徴とする。

【0022】

また、請求項8の発明は、

請求項3から請求項6の何れか1つの記憶装置であって、

さらに、光検知回路を備え、

上記読み出しデータ制御回路、または上記マスク回路は、上記光検知回路によって所定の強度の光が検出されたときにだけ、上記メモリから読み出されたデータを出力するように構成されたことを特徴とする。

【0023】

これらによると、検知される温度や光の強度が適切でない場合にも、記憶データがマイクロコンピュータに取り込まれないようにすることができるので、不正確な情報の取得を一層容易に防止することができる。

【0024】

また、請求項9の発明は、

メモリとマイクロコンピュータとを備え、外部から入力されるクロック信号に応じて、上記メモリに記憶されたデータが上記マイクロコンピュータに取り込まれるように構成された記憶装置において、

上記メモリから読み出されたデータを、所定の期間だけ、上記マイクロコンピュータへ出力するマスク回路と、

上記マスク回路が上記メモリから読み出されたデータを出力する上記所定の期間、および上記マイクロコンピュータが上記マスク回路から出力されたデータを取り込むタイミングを可変に制御するタイミング制御回路と、
を備えたことを特徴とする。

【0025】

また、請求項10の発明は、

請求項9の記憶装置であって、

上記タイミング制御回路は、

上記マスク回路が上記メモリから読み出されたデータを出力する上記所定の期

間、および上記マイクロコンピュータが上記マスク回路から出力されたデータを取り込むタイミングを、

上記メモリにおける所定の領域に保持されたデータ、

上記マイクロコンピュータから出力されるアドレス、および

上記マイクロコンピュータから出力される所定の信号の少なくとも何れか1つに基づいて設定するように構成されたことを特徴とする。

【0026】

これらによれば、メモリがアクセスされるごとに、記憶データがマイクロコンピュータに入力されるタイミングが異なるので、記憶装置を分解し、記憶データの伝送経路にプローブを当てて解析するのを困難にすることができ、やはり、記憶装置に記憶されたデータの秘匿性を高くすることが容易にできる。

【0027】

【発明の実施の形態】

以下、本発明の実施の形態に係る記憶装置としてのＩＣカードについて、図面を参照しながら説明する。

【0028】

（実施の形態1）

図1は実施の形態1のＩＣカード100の全体構成を示すブロック図である。

【0029】

同図において、

マイクロコンピュータ110（プロセッサ）は、後述する半導体記憶部120から読み出されたデータを取り込むレジスタ111を備え、外部から入力されるクロック信号またはこれを分周やてい倍して得られるクロック信号に応じて、ＩＣカード100に対するデータの入出力制御や種々のデータ処理等をするものである。より詳しくは、半導体記憶部120に記憶されたプログラム等を実行することにより、外部から入力されたデータを半導体記憶部120に書き込んだり、半導体記憶部120から読み出したデータや所定の処理を施したデータを外部に出力したりするようになっている。

【0030】

上記半導体記憶部120は、マイクロコンピュータ110が実行するプログラムや種々のデータを記憶するもので、メモリアレイユニット121（メモリ）、センスアンプ122、出力バッファ123、データマスク部124（読み出しデータ制御回路）、データマスク信号発生回路125（タイミング信号出力回路）およびアクセス制御回路126を備えている。

【0031】

上記メモリアレイユニット121は、実際にプログラムやデータを保持するもので、アクセス制御回路126から出力されるロウアドレスおよびカラムアドレスに基づいて、ロウデコーダ121aおよびカラムデコーダ121bによって指定されるメモリアレイ121cの領域に対して、データの書き込みや読み出しが行われるようになっている。

【0032】

センスアンプ122は、上記メモリアレイ121cから出力される電圧を増幅し、ロウデコーダ121aおよびカラムデコーダ121bによって指定される領域に記憶されているデータ（0または1）に応じたH（High）レベルまたはL（Low）レベルのデータ信号を出力するものである。

【0033】

出力バッファ123は、センスアンプ122から出力されるデータ信号をラッピングし、安定した信号を出力するようになっている。

【0034】

データマスク部124は、データマスク信号発生回路125から出力されるデータマスク信号に応じて、出力バッファ123から入力されたデータ信号の出力の有無を制御するものである。このデータマスク部124は、具体的には、例えば図2に示すようにデータのビット数に応じた数のAND回路124aを備えて構成されている。なお、AND回路124aに代えて、出力バッファ123からの出力信号とLレベルの信号とをデータマスク信号に応じて選択的に切り替えるセレクタ（スイッチ）を設けて構成するなどしてもよい。

【0035】

データマスク信号発生回路125は、例えば図3に示すように、クロック信号

が分周（または4倍）された読み出し制御信号における立ち下がりエッジから時間 t_1 だけずれたタイミング T_3 から、タイミング T_5 までの時間 t_2 の期間だけHレベルになるデータマスク信号を出力するようになっている。ここで、上記時間 t_1 ， t_2 は、適正なクロック信号の周期を t_{clk} とすると、あらかじめ

$$t_1 < t_{clk} < t_1 + t_2$$

となるように設定されている。

【0036】

アクセス制御回路126は、マイクロコンピュータ110によるメモリアレイユニット121へのアクセスを制御するものである。より詳しくは、例えば、マイクロコンピュータ110から出力される読み出し制御信号、モード信号、およびアドレス信号に基づいて、ロウアドレス信号およびカラムアドレス信号や、センスアンプ122の動作を制御する動作制御信号、ラッチ信号、および種々の読み出しモードなどを設定する図示しないモード制御信号を出力するようになっている。

【0037】

なお、通常は、さらに、メモリアレイユニット121にデータを書き込むための回路等も設けられているが、説明の便宜上、ここでは省略する。

【0038】

上記のように構成されたICカードにおける、メモリアレイユニット121に記憶されたデータの読み出し動作について簡単に説明すると、例えば、1回の読み出し動作は、クロック信号の2周期分のタイミングに対応して行われる。また、アクセス制御回路126から出力される読み出し制御信号は、最初の1周期の期間にLレベルになり、この期間にだけセンスアンプ122は動作状態になる。この動作状態のセンスアンプ122から出力されるデータ信号は、出力バッファ123によって、2周期目の終わりのタイミングまでラッチされる。出力バッファ123の出力はデータマスク部124によってマスクされ、前記のように所定の $T_3 \sim T_5$ の期間だけ、有効なデータ信号が出力される。マイクロコンピュータ110は、1周期目の終わりにクロック信号が立ち下がるタイミングで、デー

タマスク部124から出力されるデータを取り込む。

【0039】

以下、より詳しい動作の説明として、クロック信号が所定の周波数のときに、メモリアレイユニット121に記憶されたデータが読み出されて、マイクロコンピュータ110からICカードの外部に出力される場合の動作を説明する。

【0040】

まず、ICカードの外部から、クロック信号が入力されるとともに、入力データとして、メモリアレイユニット121内のデータをそのまま外部に出力させるモードを示す制御データ、および読み出しアドレスを指定するアドレスデータが入力される。

【0041】

そこで、マイクロコンピュータ110は、例えば図3に示すタイミングT0で、読み出しモードを示すモード信号とアドレス信号とをアクセス制御回路126に出力する。これに応じて、アクセス制御回路126は、ロウデコーダ121aおよびカラムデコーダ121bに、ロウアドレス信号およびカラムアドレス信号を出力し、メモリアレイ121cにおけるデータを読み出す領域を指定する。

【0042】

次に、マイクロコンピュータ110は、クロック信号が立ち下がるタイミングT1で、読み出し制御信号をLレベルにする。そこで、アクセス制御回路126は、センスアンプ122に動作制御信号（電源電圧または接地電圧）を出力し、センスアンプ122は、動作状態になって、ある程度の期間の不定状態を経た後（タイミングT2）、メモリアレイユニット121の記憶内容に応じたレベルの信号を出力する。出力バッファ123は、センスアンプ122から出力されたレベルの信号をそのまま出力する。

【0043】

アクセス制御回路126は、また、上記センスアンプ122の出力が安定する上記タイミングT2以降の所定のタイミングで、出力バッファ123に出力するラッチ信号を例えばHレベルにし、出力バッファ123は、その時点でセンスアンプ122から出力されている信号のレベルを保持する。すなわち、アクセス制

御回路126からの動作制御信号の出力は読み出し制御信号がHレベルになるタイミングT4で停止されてセンスアンプ122の出力は不定な状態になるが、出力バッファ123は、例えば次に読み出し制御信号がLレベルになるタイミングT6まで、メモリアレイユニット121の記憶内容に応じたレベルのデータ信号を出力し続ける。

【0044】

また、データマスク信号発生回路125は、読み出し制御信号の立ち下がり（T1）から所定の時間t1だけ経過した後、時間t2の間（T3～T5）だけ、データマスク信号をHレベルにする。そこで、データマスク部124は、上記タイミングT3～T5の期間だけ、出力バッファ123に保持されているデータ信号を出力する。

【0045】

一方、マイクロコンピュータ110は、クロック信号が立ち下がるタイミングT4で、データマスク部124から出力されているデータ信号、すなわちメモリアレイユニット121から読み出されたデータを取り込み、内部でデータの処理を行った後、ICカードの外部に出力する。すなわち、クロック信号の周波数が、その周期（T1～T4）がt1～t1+t2の範囲となるような周波数である場合には、記憶データが適切にマイクロコンピュータ110に取り込まれ、ICカードの外部に出力される。

【0046】

ところが、クロック信号の周波数が上記のような範囲にない場合、例えば図4に示すようにクロック信号の周期がt1+t2よりも長い場合には、クロック信号が立ち下がるタイミングT4では、データマスク部124は、記憶データに係らずLレベルの信号を出力しているので、マイクロコンピュータ110は、このLレベルの信号を取り込んでしまう。したがって、記憶データは、ICカードから外部へ出力されることはない。（なお、実際には、マイクロコンピュータ110が実行する命令コードも同様にメモリアレイユニット121から適切に読み出されないので、マイクロコンピュータ110の動作自体も適切に行われないことになる。）

ここで、一般に、クロック信号に同期して動作するデジタル回路は、クロック信号の周波数を低くしても適切に動作する。このため、通常、第3者が不正にICカードを解析して記憶内容を読み取ろうとするような場合には、回路動作を遅くして解析を容易にするために、低い周波数のクロック信号を与えることが多い。しかしながら、上記のように所定のクロック信号の周波数でだけマイクロコンピュータ110に記憶データが読み出されるようにすることにより、データの不正取得等を容易に防止することができる。

【0047】

なお、データマスク信号がHレベルになる期間は、1回に限らず、複数回生じるようにもよい。この場合には、複数種類のクロック信号周波数に対して適切な動作をさせることができるので、例えばICカードに高速な動作をさせるモードと低消費電力な動作をさせるモードとでクロック信号周波数を切り替えるような場合に、何れのモードでも適切な動作をさせ、かつ、その他の周波数では適切に動作しないようにすることができる。

【0048】

また、上記のように、クロック信号のエッジからずれたタイミングでデータマスク部124から記憶データが出力されるのに限らず、データマスク部124（マスク回路）からの記憶データの出力開始または停止のいずれか一方のタイミングをクロック信号のエッジに同期させるとともに、マイクロコンピュータ110による記憶データの取り込みタイミングが、クロック信号のエッジから所定の時間だけずれたタイミングになるようにしたり、さらに、記憶データの出力開始および停止、取り込みの何れもクロック信号のエッジからずれたタイミングになるようにしたりしても、同様の効果を得ることができる。

【0049】

また、上記のようなデータマスク信号がHレベルである期間に、クロック信号のエッジが存在する場合には、データマスク部から記憶データを出力させる一方、存在しない場合には記憶データが出力されないようにしても、やはり、所定のクロック信号の周波数のときにしかマイクロコンピュータ110に記憶データが取り込まれないようにすることができる。

【0050】

また、本実施の形態のような手法は、単独で用いるのに限らず、例えば暗証番号との照合をする手法や記憶データ自体を暗号化する手法など、公知の種々の手法と組み合わせて、より秘匿性を高め得るようにしてよい。

【0051】**(実施の形態2)**

以下、実施の形態2のICカードについて説明する。なお、以下の実施の形態において、前記実施の形態1等と同様の機能を有する構成要素については同一の符号を付して説明を省略する。

【0052】

実施の形態2のICカードは、図5に示すように、前記実施の形態1のICカードと比べて、データマスク部124に代えて、データマスク部224を備えるとともに、さらに、ランダムデータ発生回路231を備えている点が異なる。

【0053】

上記ランダムデータ発生回路231は、所定のタイミングでランダムなデータ信号を出力するようになっている。

【0054】

また、データマスク部224は、具体的には、例えば図6に示すように、データのビット数に応じた数のセレクタ224aを備えて構成されている。

【0055】

上記のように構成されていることにより、例えば図7に示すように、データマスク部224からは、データマスク信号がHレベルの場合には、前記実施の形態1と同様にメモリアレイユニット121から読み出されたデータ信号が出力される一方、データマスク信号がLレベルの場合には、ランダムデータ発生回路231から出力されるランダムデータ信号が出力される。

【0056】

すなわち、クロック信号周波数が適切な場合には、ランダムデータ発生回路231から出力されるランダムデータ信号に係らず、マイクロコンピュータ110は、メモリアレイユニット121から読み出された信号がデータマスク部224

から出力されているタイミングで、そのデータ信号を取り込み、適切に動作する。一方、例えばクロック信号の周波数が低い場合には、図8に示すように、マイクロコンピュータ110はデータマスク部124から出力されるランダムデータ信号を取り込むことになるので、適切に動作しないことになる。

【0057】

また、例えば第3者がICカードを分解し、LSIチップや配線パターンにプローブを当ててICカード内部の信号を解析するような場合でも、記憶データとランダムデータとの区別がつきにくいので、実際上、メモリアレイユニット121の記憶内容を不正に取得することが困難になる。さらに、仮に適切な周波数のクロック信号が与えられてマイクロコンピュータ110が正常に動作する場合でも、ICカードの内部でだけ用いられて外部に出力されないようなデータ（プログラムによってそのように扱われるデータ）は、ランダムデータとの区別がつきにくい以上、やはり不正に読み取ることは困難になる。

【0058】

ここで、上記ランダムデータとしては、厳密な意味でのランダム性の高いデータである必要は必ずしもなく、記憶データとは異なるが紛らわしいダミーデータであればよい。したがって、例えば、記憶データやアドレスなどのビット位置を入れ替えたものや、これらに所定の変換を施したものなどを用いてもよい。

【0059】

また、ランダムデータが変化する周期は特に限定されないが、データマスク信号がHレベルになる期間と対応させる方が、より記憶データとの識別が困難になるので好ましい。

【0060】

(実施の形態3)

実施の形態3のICカードは、図9に示すように、前記実施の形態2のICカードと比べて、さらに、温度検知回路331を備えるとともに、データマスク信号発生回路125に代えて、上記温度検知回路331によって所定の範囲の温度が検知された場合にだけ、実施の形態2と同じタイミングでデータマスク信号をHレベルにするデータマスク信号発生回路325を備えている点が異なる。

【0061】

上記のような温度検知回路331とデータマスク信号発生回路325とが設けられることによって、所定の温度範囲で、かつ、所定の周波数のクロック信号が与えられた場合にだけ、マイクロコンピュータ110が正常に動作し、その他の場合には記憶データが読み出されないので、一層、記憶データの秘匿性を高めることが容易にできる。

【0062】

さらに、前記のようにICカードを分解、解析されたとしても、温度範囲が適切でない場合には、データマスク部124とマイクロコンピュータ110との間の信号線（データバス）では記憶データが全く伝送されないので、プローブを当てて解析されるようなことも一層容易に防止できる。

【0063】

ここで、メモリアレイユニット121からデータマスク部124までの間では、記憶データが伝送されるが、メモリアレイユニット121から出力バッファ123の間では、通常、伝送される信号は微弱であったり出力インピーダンスが高かったりするので、プローブを当てるなどして信号を検出すること自体が困難である。また、メモリアレイユニット121からデータマスク部124までの回路は、通常密接して形成されるので、回路を解析してデータ信号の経路であることを認識することが困難であるうえ、物理的にプローブを当てることも容易ではない。それゆえ、上記のようにデータマスク部124とマイクロコンピュータ110との間、すなわち、データバスであることが配線パターンなどから比較的容易に認識され、また配線長が比較的長くてプローブが当たれやすい信号経路に、ランダムデータ信号だけが出力される（記憶データが出力されない）ようにすることによって、実際上、秘匿性をかなり高めることができる。

【0064】

なお、データマスク信号発生回路325がHレベルのデータマスク信号を出力するための条件としては、上記のように単に所定の範囲の温度が検知されることだけでなく、例えば高温、低温、高温と変化したことが検知されることなどを条件とするようにしてもよい。

【0065】

また、データマスク部124から記憶データが出力されないようにするのに代えて、マイクロコンピュータ110において、データマスク部124から出力される記憶データの取り込みが阻止されるようにしてもよい。

【0066】

(実施の形態4)

前記実施の形態3の温度検知回路331に代えて、図10に示すように光検知回路431を設け、検出される光の強度に応じて、データマスク信号がHレベルになるようにしても、やはり同様に記憶データの秘匿性を高めることが容易にできる。

【0067】

また、光強度に関しても、所定のパターンの光強度変化に応じて、データ信号がデータマスク部124から出力されるようにしてもよい。さらに、上記のような温度検知と光検知とを組み合わせて用いるなどしてもよい。

【0068】

(実施の形態5)

実施の形態5のICカードは、図11に示すように、前記実施の形態1のICカードと比べて、データマスク信号発生回路125に代えてデータマスク信号発生回路525を備えるとともに、さらに、アドレス演算回路531を備えている点と、マイクロコンピュータ110が、アドレス演算回路512と、ラッチ信号発生回路513とを備えている点が異なる。

【0069】

上記アドレス演算回路531は、マイクロコンピュータ110から出力されるアドレス信号に基づいて所定の演算等（何もしない場合も含む）を行い、その演算結果をデータマスク信号発生回路525に出力するようになっている。具体的には、例えば、アドレスのLSBの値や、所定の複数ビットの値、また、これらに所定の変換を施した値などを出力するようになっている。なお、アクセス制御回路126から出力されるロウアドレスやカラムアドレスに基づいて演算を行うようにしてもよい。

【0070】

データマスク信号発生回路525（タイミング制御回路）は、データマスク部124（マスク回路）による読み出しデータ信号の出力タイミングを制御する点では実施の形態1と同じであるが、クロック信号の立ち下がりエッジからデータマスク信号がHレベルになるまでの時間t1、およびデータマスク信号がHレベルになっている時間t2の少なくとも何れか一方が、上記アドレス演算回路531から出力される演算結果に基づいて設定されるようになっている。すなわち、前記実施の形態1のICカードでは、上記時間t1、t2はあらかじめ設定された一定の長さであるのに対し、本実施の形態のICカードでは、データマスク信号がHレベルになるタイミングは、メモリアクセスごとに、そのアクセスするアドレスに応じて変化するようになっている。

【0071】

また、マイクロコンピュータ110のアドレス演算回路512は、上記アドレス演算回路531と同じ演算を行うように構成され、ラッチ信号発生回路513（タイミング制御回路）は、アドレス演算回路512から出力される演算結果に基づいて、レジスタ111にラッチ信号を出力するように構成されている。上記ラッチ信号発生回路513は、より詳しくは、アドレス演算回路512の演算結果に基づいて、時間t2の期間内、すなわちデータマスク信号がHレベルである期間内のタイミングで上記ラッチ信号のレベルを変化させる（エッジを生じさせる）ようになっている。

【0072】

上記のように構成されたICカードでは、データマスク信号とマイクロコンピュータ110内のラッチ信号とは、タイミングが常に対応することになるので、マイクロコンピュータ110は、クロック信号の周波数に係らず正常に動作することになるが、データマスク部124から適切な記憶データが出力されるタイミングは、メモリアクセスごとに変化するため、データマスク部124とマイクロコンピュータ110との間の信号線（データバス）にプローブを当てることによる解析などを困難にすることができる。

【0073】

(実施の形態6)

実施の形態6のICカードは、図12に示すように、メモリアレイユニット121内の所定の領域に、データマスク信号がHレベルになるタイミング（時間t1, t2）に応じたマスクタイミングデータを格納することによって、時間t1, t2やマイクロコンピュータ110による取り込みタイミングを設定し得るようとしたものである。

【0074】

具体的には、実施の形態5のICカードに比べ、アドレス演算回路531およびデータマスク信号発生回路525に代えて、データマスク信号発生回路625を備えている点と、マイクロコンピュータ110が、アドレス演算回路512およびラッチ信号発生回路513に代えて、ラッチ信号発生回路613を備えている点とが異なる。

【0075】

上記データマスク信号発生回路625（タイミング制御回路）には、アドレス信号と、出力バッファ123から出力されるデータ信号とが入力され、メモリアレイユニット121における所定のアドレスの領域がアクセスされたときに、出力バッファ123から出力されるマスクタイミングデータに基づいて、上記時間t1, t2が設定され、データマスク部124（マスク回路）が制御されるようになっている。

【0076】

また、マイクロコンピュータ110のラッチ信号発生回路613（タイミング制御回路）には、アドレス信号と、データマスク部124から入力されるデータ信号とが入力され、上記データマスク信号発生回路625で時間t1, t2が設定されるのに対応して、レジスタ111に出力されるラッチ信号のエッジタイミングが設定されるようになっている。

【0077】

上記のように構成されることにより、データマスク部124から適切な記憶データが输出されるタイミングを柔軟に設定することができるので、やはり、データバスにプローブを当てることによる解析などを一層困難にすることができます。

【0078】

なお、上記マスクタイミングデータは、複数格納されて選択的に用いられるようにもよい。

【0079】

(実施の形態7)

実施の形態7のICカードは、図13に示すように、実施の形態5のICカードに比べて、アドレス演算回路512, 531に代えて、タイミング制御部714（タイミング制御回路）を備え、ラッチ信号発生回路513およびデータマスク信号発生回路525は、上記タイミング制御部714からの出力に基づいて、データマスク信号がHレベルになるタイミングや、マイクロコンピュータ110のレジスタ111がデータマスク部124（マスク回路）から出力されたデータ信号を取り込むタイミングを制御するようになっている。

【0080】

上記タイミング制御部714は、具体的には、例えば記憶データが読み出されるごとや、マイクロコンピュータ110が動作を開始する際などに、乱数などを出力するようにしたり、プログラムによって決定される値を出力するようにしたりしてもよいし、また、ICカードごとに設定された値を出力するようにしてもよい。

【0081】

これによっても、やはり前記実施の形態6、7と同様に、データバスにプローブを当てるによる解析などを一層困難にして、記憶データの秘匿性を高めることができる。

【0082】

なお、上記の例では、メモリとマイクロコンピュータとを備えた記憶装置の例としてICカードを例に挙げて説明したが、これに限らず、いわゆるタグ型の記憶装置などであってもよいし、また、ホスト装置との接続が接続端子を接触させることによって行われる接触型であってもよいし、電磁波によって行われる非接触型であってもよい。

【0083】

また、上記各実施の形態や変形例の構成は、論理的に可能な範囲で種々組み合わせるようにしてもよい。具体的には、例えば実施の形態3～7のようにランダムデータ信号が出力されるのに代えて、実施の形態1のようにL（またはH）レベルの信号が出力されるようにしてもよいし、また、実施の形態3、4のように温度検知回路331や光検知回路431を実施の形態5～7の構成にも設けるなどしてもよい。

【0084】

【発明の効果】

以上のように、本発明によると、クロック信号が所定の周波数のときにだけ、メモリから読み出されたデータが、マイクロコンピュータに取り込まれるようになしたり、上記取り込みタイミングを可変にしたりすることによって、第3者による記憶データの不正な読み出しや解析を困難にすることができるので、ICカード等の記憶装置の秘匿性を高めることができ一方、所定の周波数のクロック信号を与えることなどによって、必要に応じて内部データを読み出すことなども容易にできる。

【図面の簡単な説明】

【図1】

実施の形態1のICカード100の全体構成を示すブロック図である。

【図2】

同、データマスク部124の具体的な構成を示す回路図である。

【図3】

同、適切なクロック周波数での動作を示すタイミングチャートである。

【図4】

同、不適切なクロック周波数での動作を示すタイミングチャートである。

【図5】

実施の形態2のICカード100の全体構成を示すブロック図である。

【図6】

同、データマスク部224の具体的な構成を示す回路図である。

【図7】

同、適切なクロック周波数での動作を示すタイミングチャートである。

【図8】

同、不適切なクロック周波数での動作を示すタイミングチャートである。

【図9】

実施の形態3のICカード100の全体構成を示すブロック図である。

【図10】

実施の形態4のICカード100の全体構成を示すブロック図である。

【図11】

実施の形態5のICカード100の全体構成を示すブロック図である。

【図12】

実施の形態6のICカード100の全体構成を示すブロック図である。

【図13】

実施の形態7のICカード100の全体構成を示すブロック図である。

【符号の説明】

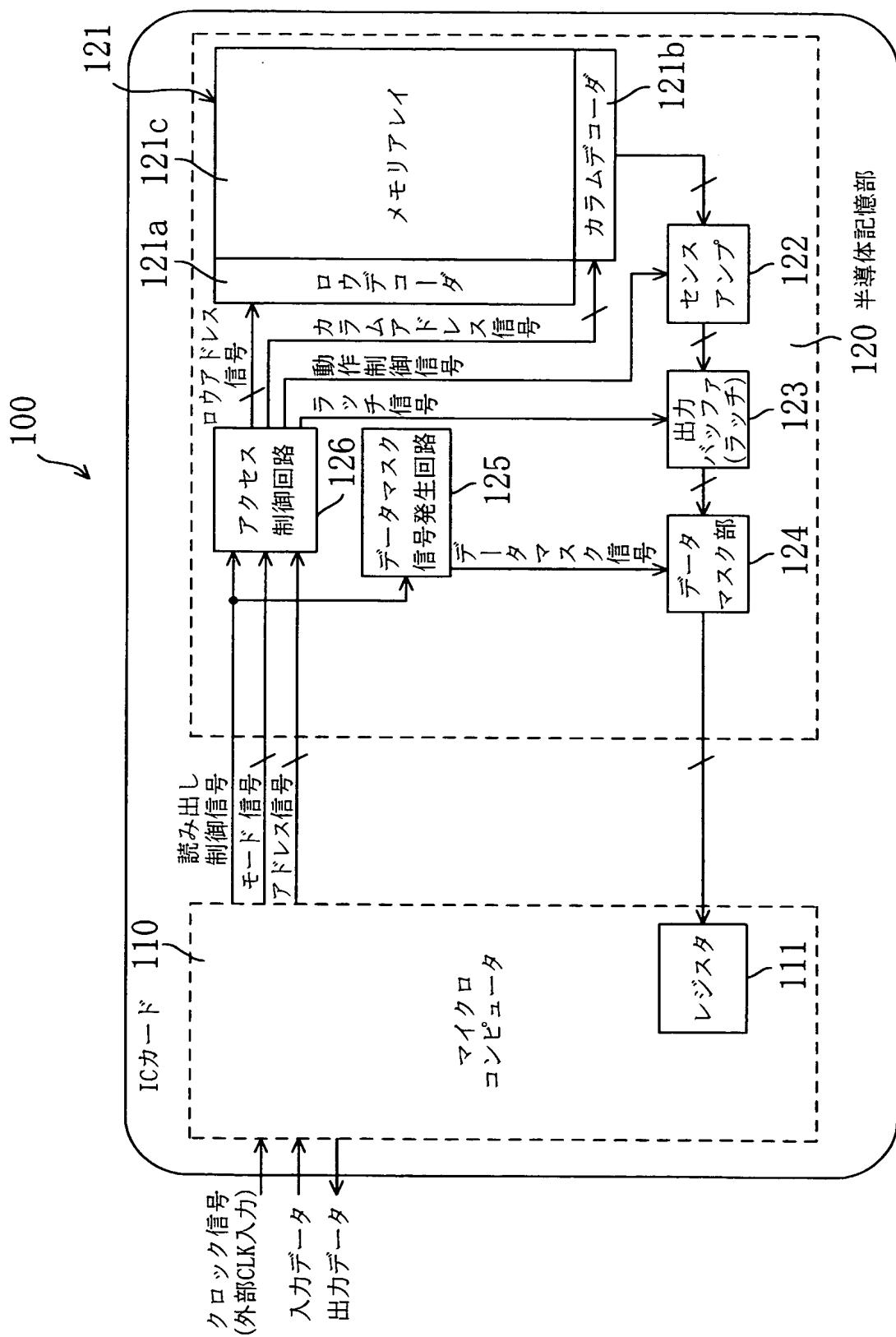
100	ICカード
110	マイクロコンピュータ
111	レジスタ
120	半導体記憶部
121	メモリアレイユニット
121a	ロウデコーダ
121b	カラムデコーダ
121c	メモリアレイ
122	センスアンプ
123	出力バッファ
124	データマスク部
124a	AND回路
125	データマスク信号発生回路
126	アクセス制御回路
224	データマスク部

224a セレクタ
231 ランダムデータ発生回路
325 データマスク信号発生回路
331 温度検知回路
431 光検知回路
512 アドレス演算回路
513 ラッチ信号発生回路
525 データマスク信号発生回路
531 アドレス演算回路
613 ラッチ信号発生回路
625 データマスク信号発生回路
714 タイミング制御部

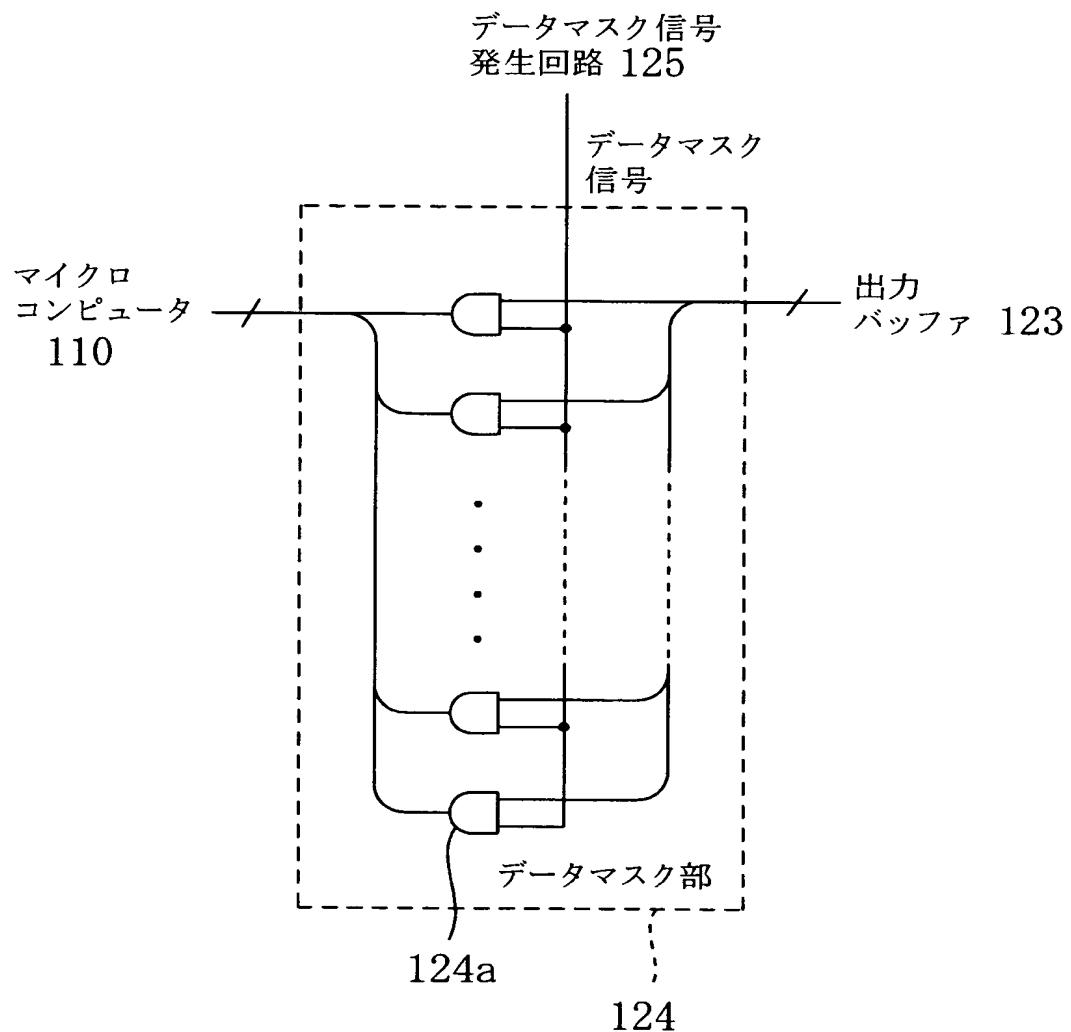
【書類名】

図面

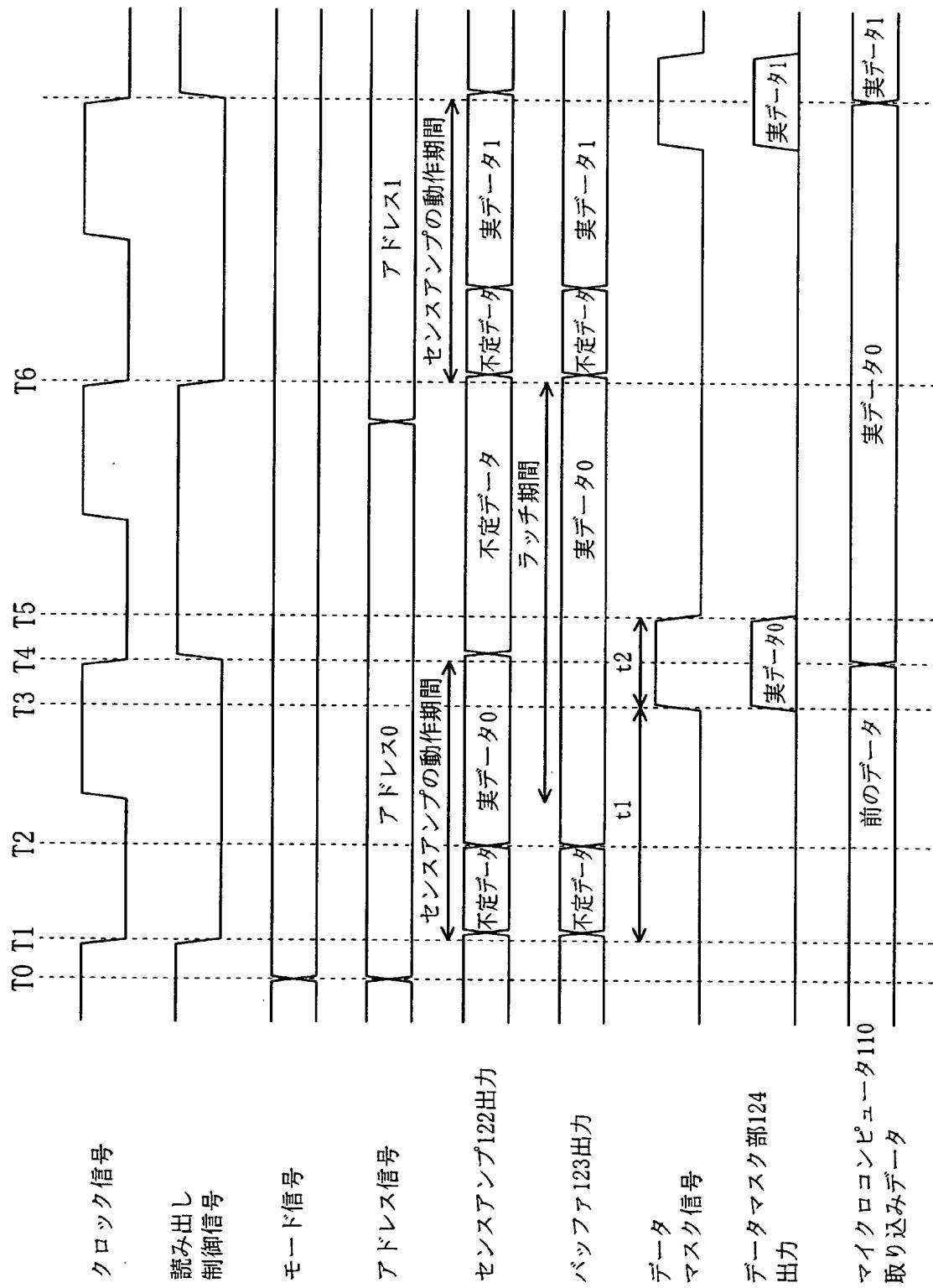
【図 1】



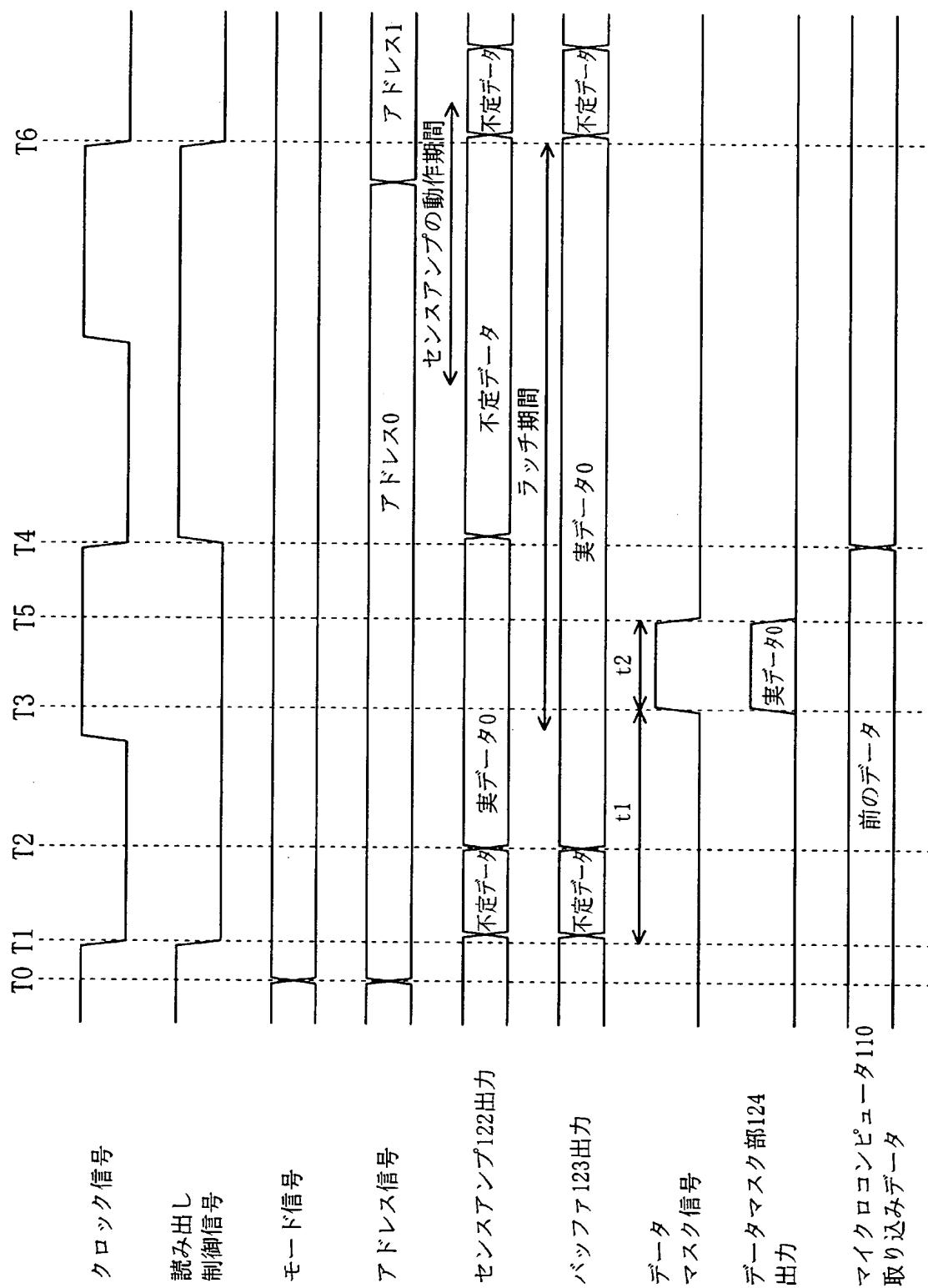
【図2】



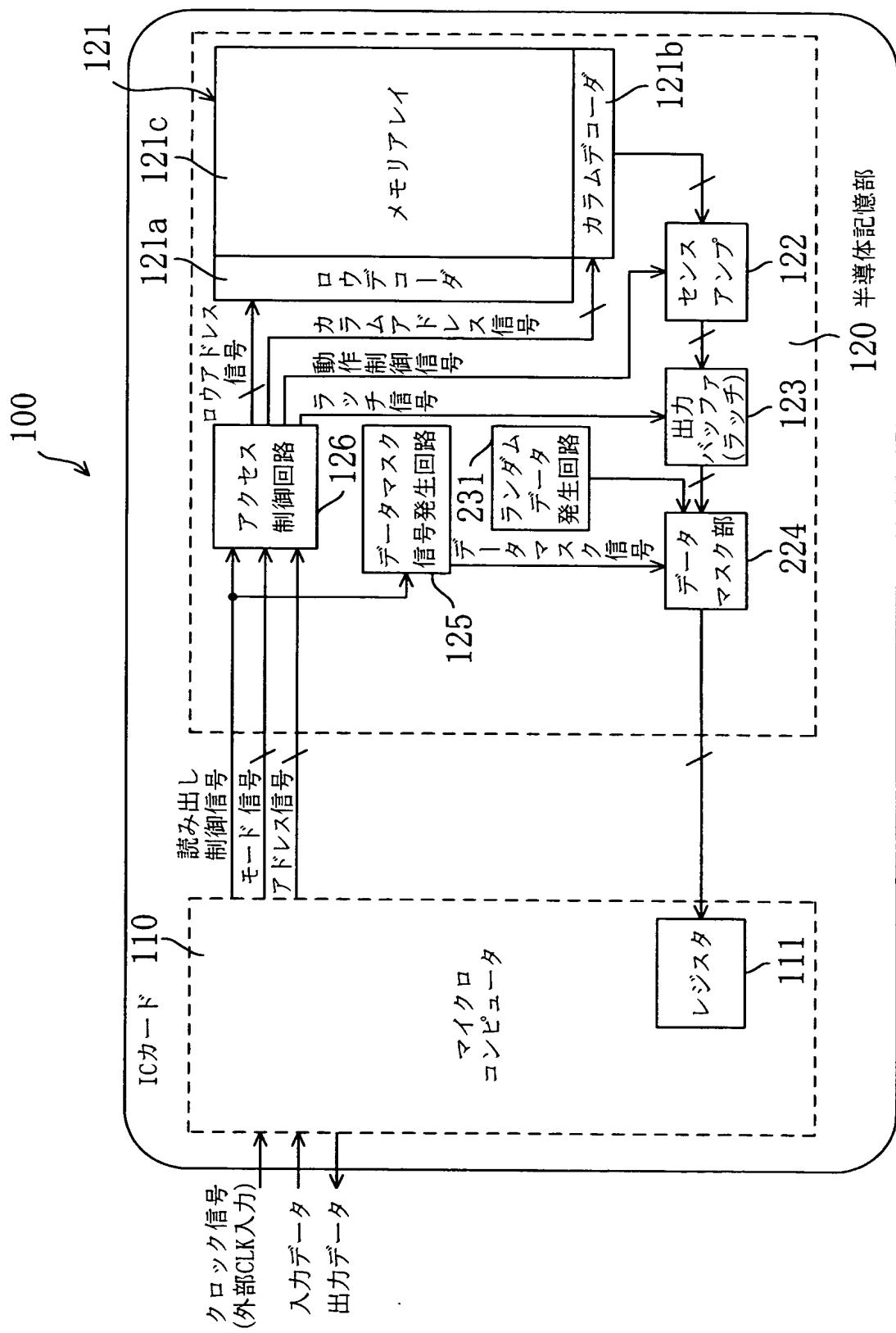
【図3】



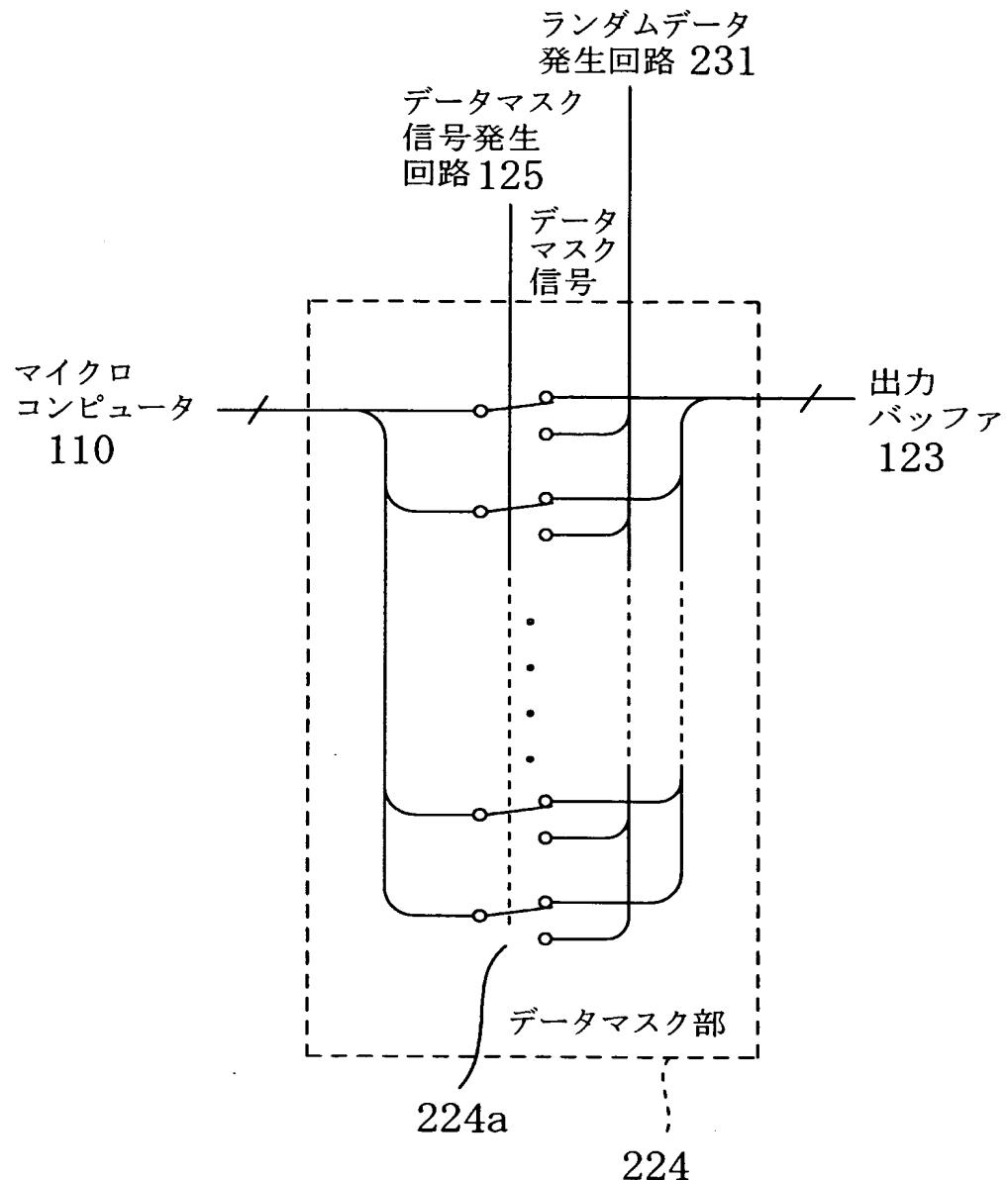
【図4】



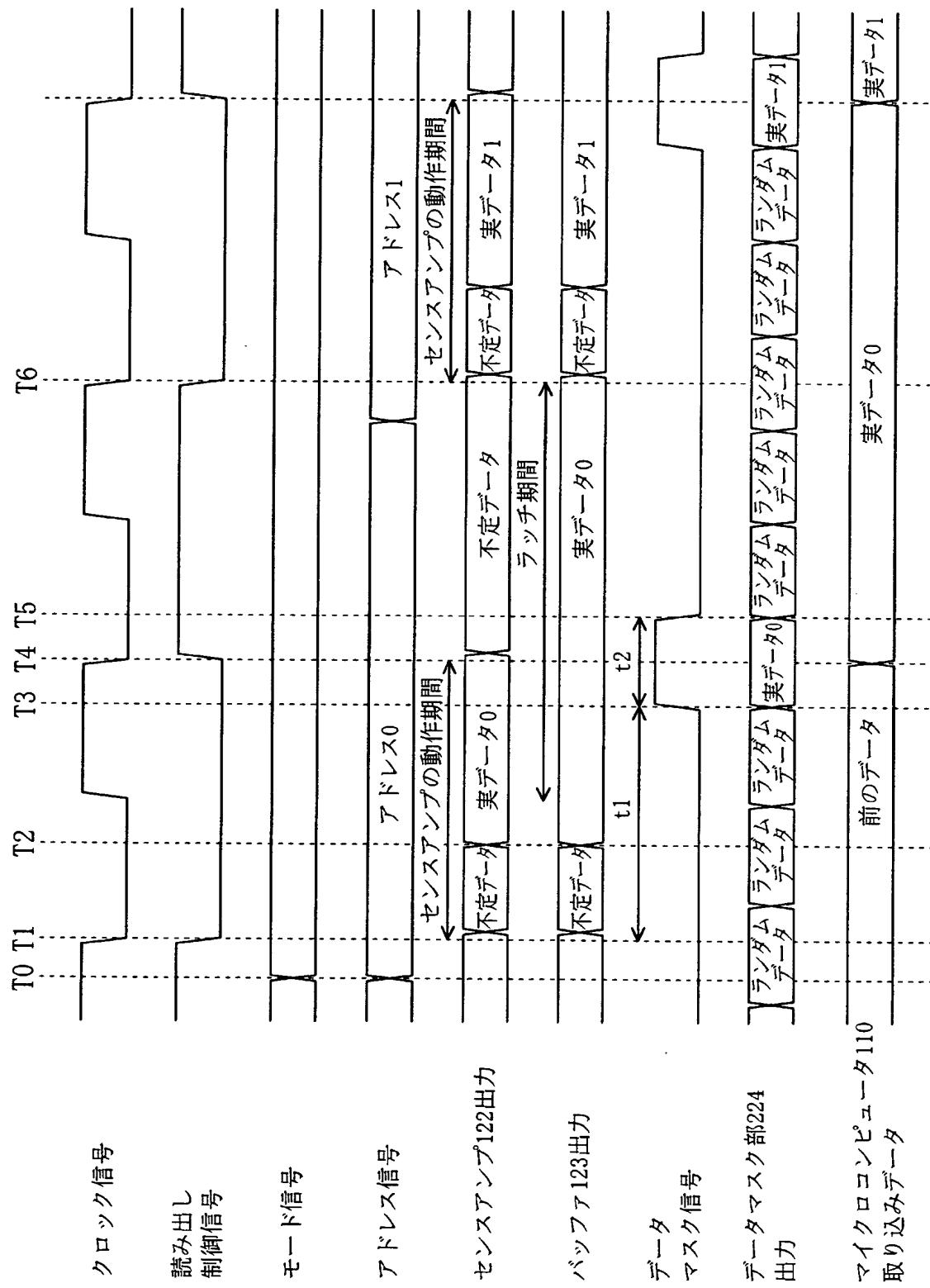
【図5】



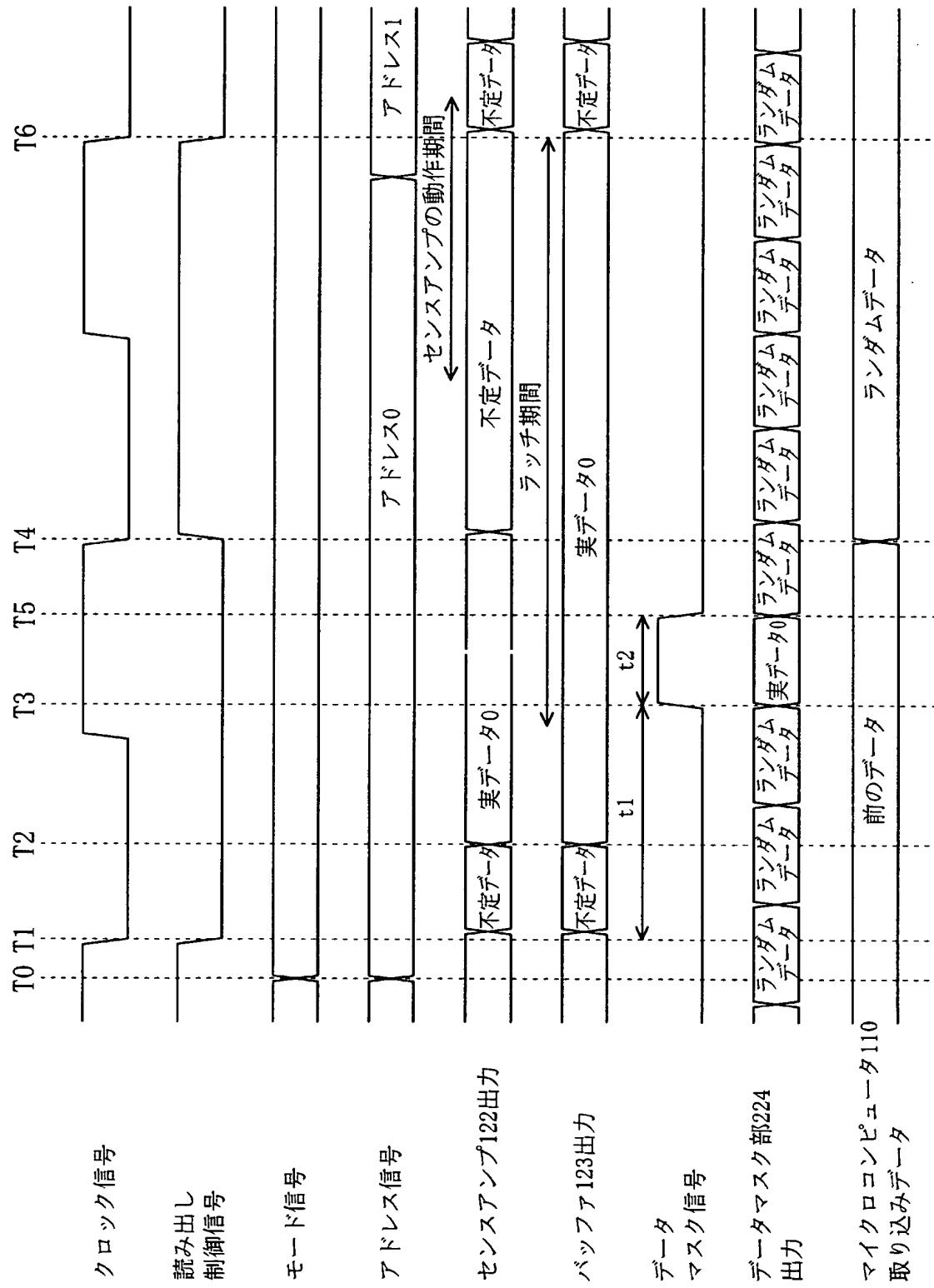
【図6】



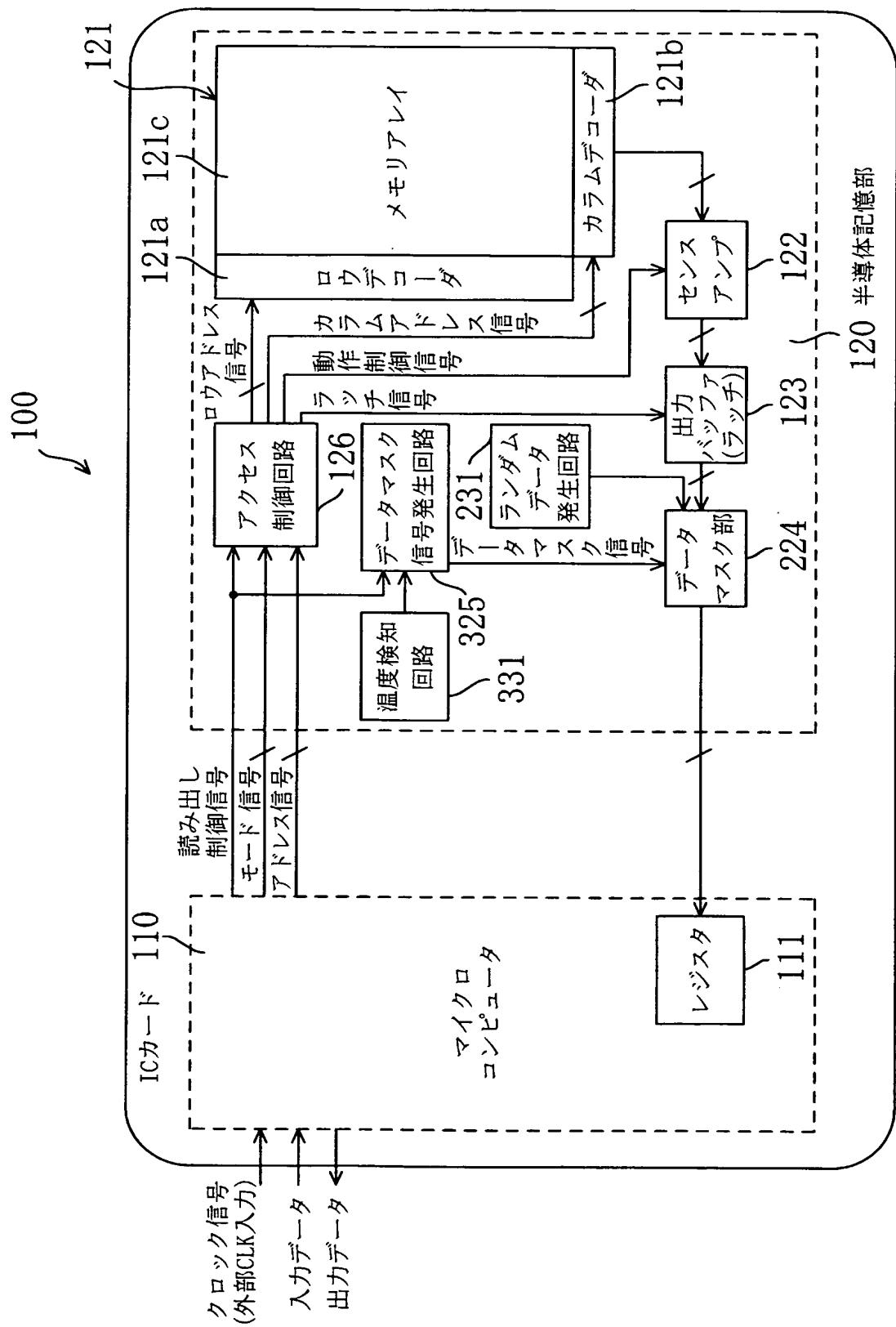
【図7】



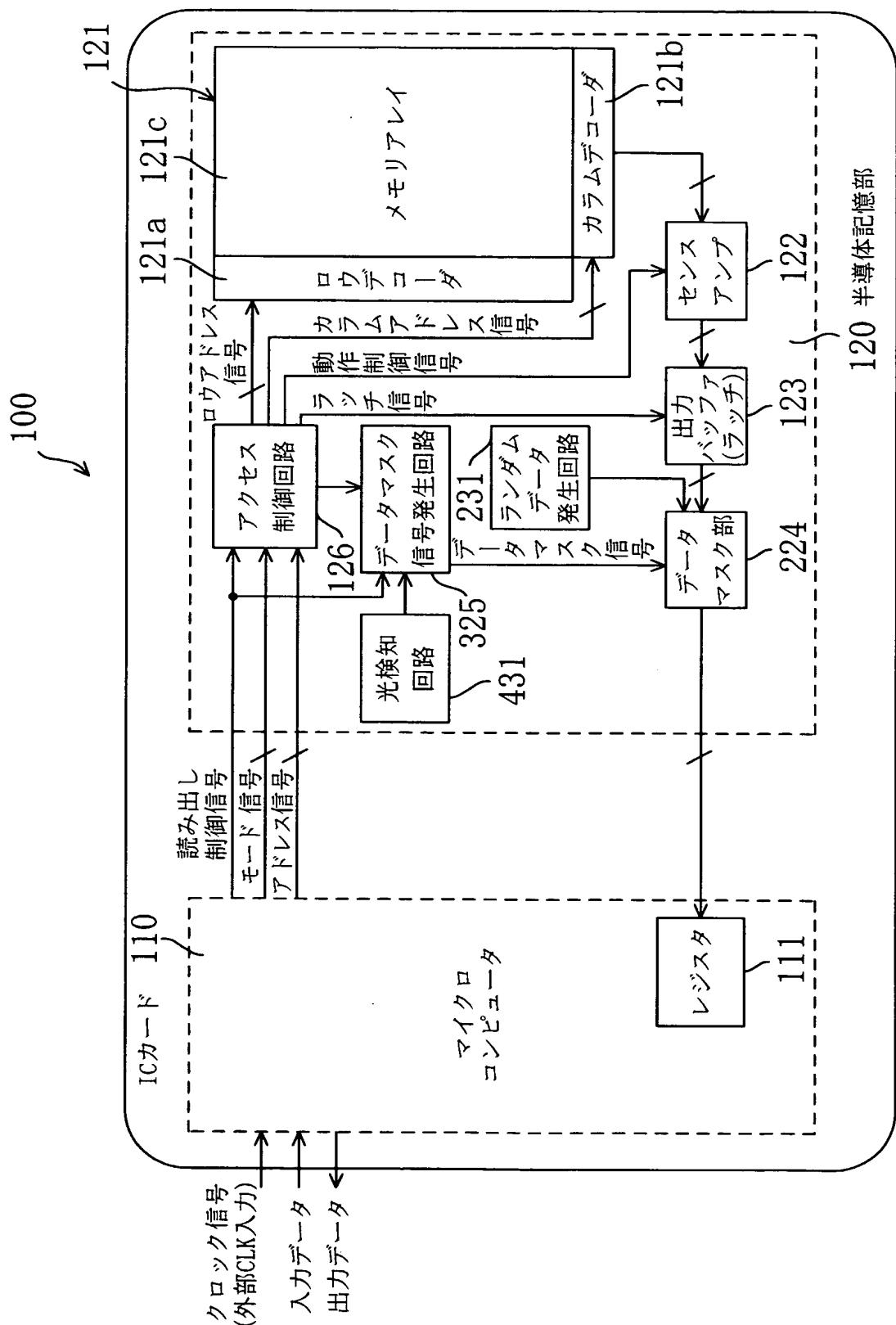
【図8】



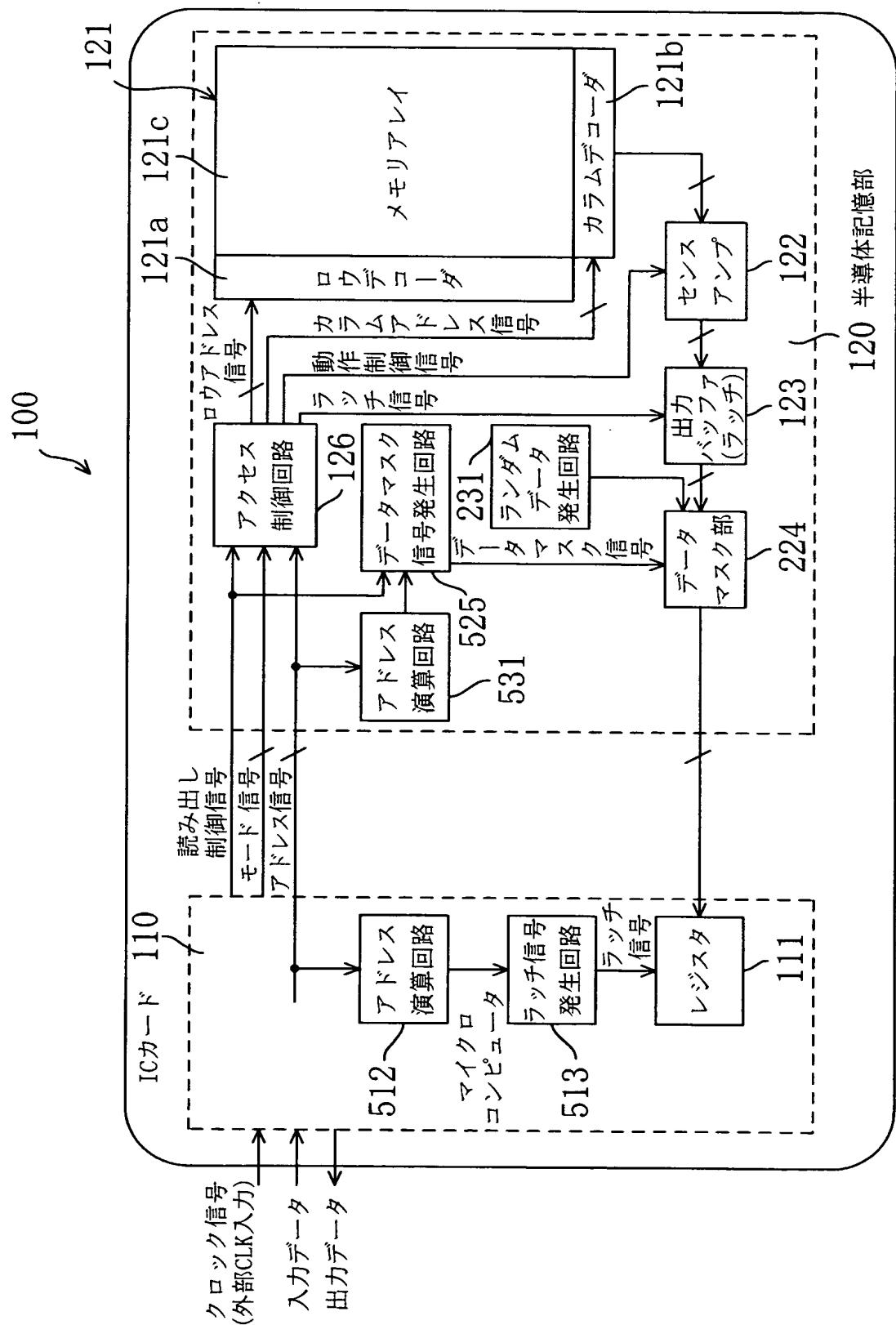
【図9】



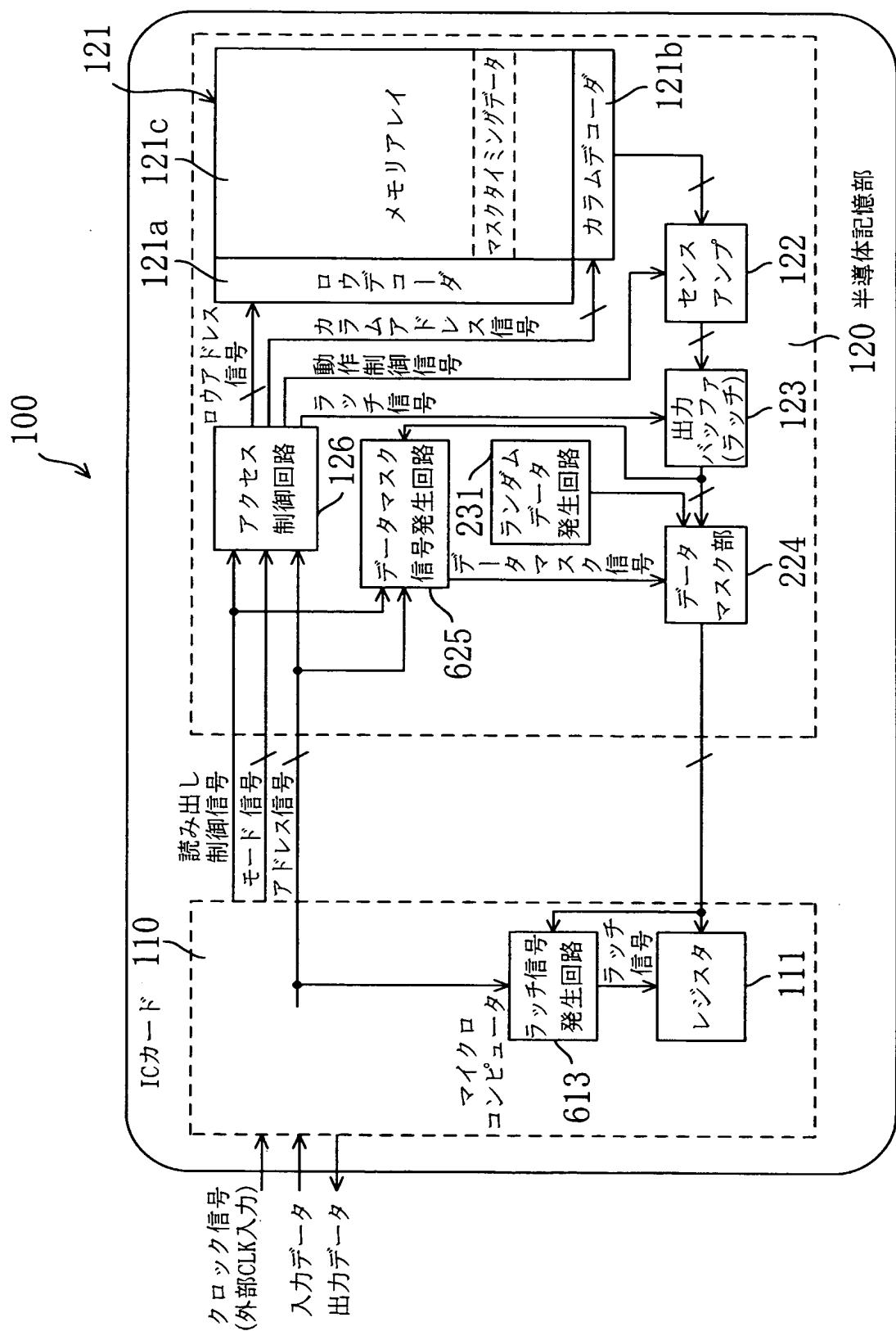
【図10】



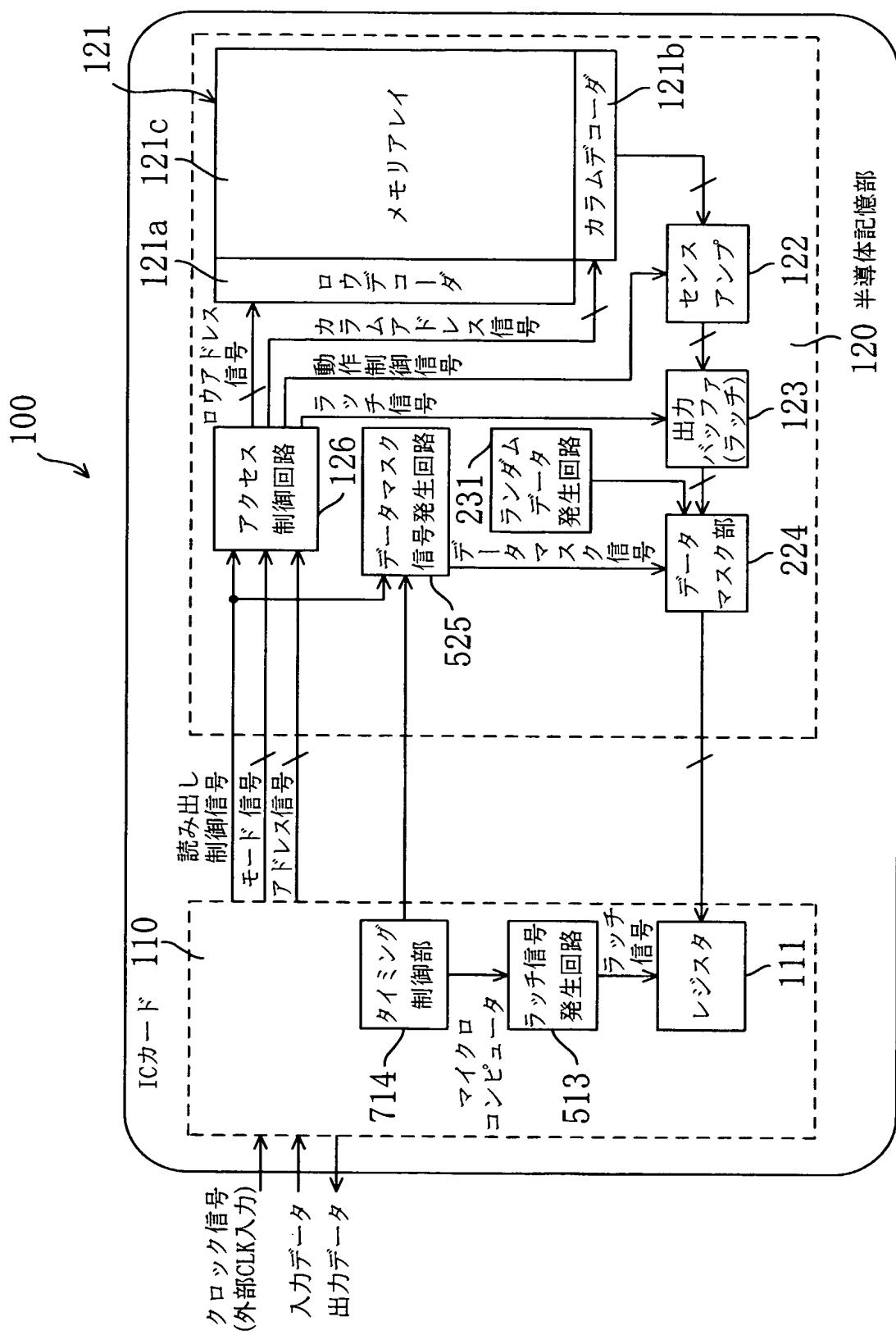
【図11】



【図12】



【図13】



【書類名】 要約書

【要約】

【課題】 I Cカードなどの記憶装置において、記憶されているデータの秘匿性を高くする。

【解決手段】 データマスク部124はメモリアレイユニット121から読み出された記憶データをクロック信号のエッジタイミングとずれた所定の期間だけ出力し、マイクロコンピュータ110はクロック信号のエッジタイミングで、データマスク部124から出力されるデータを取り込む。それゆえ、クロック信号の周波数が所定の範囲にある場合にしか、マイクロコンピュータ110は記憶データを適切に取り込むことができないので、不正な記憶データの取得を困難にすることができます。また、上記所定の期間以外にデータマスク部124からランダムデータなどが出力されるようすれば、一層、記憶データの解析を困難にして秘匿性を高くすることができます。

【選択図】 図1

特願2002-348774

出願人履歴情報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住所 大阪府門真市大字門真1006番地
氏名 松下電器産業株式会社